Symmetry implies independence

Renato Renner
Department of Applied Mathematics and Theoretical Physics
University of Cambridge, UK
r.renner@damtp.cam.ac.uk

Given a quantum system consisting of many parts, we show that *symmetry* of the system's state, i.e., invariance under swappings of the subsystems, implies that almost all of its parts are virtually *identical* and *independent* of each other. This result generalises de Finetti's classical representation theorem for infinitely exchangeable sequences of random variables as well as its quantum-mechanical analogue. It has applications in various areas of physics as well as information theory and cryptography. For example, in experimental physics, one typically collects data by running a certain experiment many times, assuming that the individual runs are mutually independent. Our result can be used to justify this assumption.

I. INTRODUCTION

In physics, properties of a large system (e.g., the universe) are typically inferred based on observations restricted to a small part of it (namely the part which is accessible to our experiments). For example, based on experiments in a laboratory showing that a hydrogen atom absorbs radiation at a certain wavelength, we naturally conjecture that the same is true for all hydrogen atoms in the universe. In other words, we expect that a limited number of local experiments is sufficient to derive general physical laws.

While this paradigm is crucial for the interpretation of experimental data, it is, however, generally impossible to provide experimental evidence in support of the paradigm itself. So, how else can it be justified? What exactly are the underlying assumptions? To answer these questions, we consider an abstract problem, in the following referred to as the *tomography problem* (cf. Fig. 1). Let $\mathcal{S}_1, \ldots, \mathcal{S}_N$ be N subsystems of a large composite system and assume that individual experiments are performed on k of the subsystems, $\mathcal{S}_1, \ldots, \mathcal{S}_k$, for $k \ll N$. The goal is to infer the physical state of the remaining $N-k$ subsystems $\mathcal{S}_{k+1}, \ldots, \mathcal{S}_N$, based on this experimental data. Note that the characteristics of the observed subsystems $\mathcal{S}_1, \ldots, \mathcal{S}_k$ might, in general, be completely unrelated to the characteristics of $\mathcal{S}_{k+1}, \ldots, \mathcal{S}_N$, in which case the observation of the former does not give any information on the latter. Hence, in order to achieve the above goal, one needs to make certain minimal assumptions on the structural properties of the overall system.

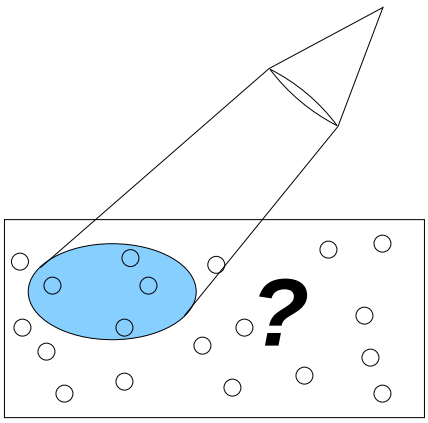

FIG. 1: Given a system consisting of many subsystems (indicated by small circles), the goal is to infer the system's characteristics based on observations of only a small part of it (oval set).

In this article, we demonstrate that, for non-relativistic quantum systems, the tomography problem can be solved under the sole assumption that the overall system is symmetric under permutations of the N subsystems. More generally, we show that any symmetric system can be analysed in the same way as if its subsystems were independent and identical copies of each other—symmetry is thus sufficient to justify the paradigm of experimental physics described at the beginning. Remarkably, symmetry of realistic systems often holds in general because of certain natural properties such as the indistinguishability of identical particles. The result thus has a wide range of applications. These include quantum information theory and cryptography, where it enables the generalisation of statements which previously have only been known to be true under certain independence assumptions.

II. INDEPENDENCE AND SYMMETRY

The physical state ρ^N of an N-partite system is said to be *independent and identically distributed (i.i.d.)* if its N parts are identical copies of some *prototype state* σ, i.e., formally, $\rho^N = \sigma^{\otimes N}$.[1] Note that, by applying only individual measurements on a certain (sufficiently large) number of subsystems, the corresponding prototype σ

[1] We adopt the density operator formalism which is commonly used in quantum mechanics. Note that the formalism also applies to purely classical systems. In this case, all density operators are diagonal with respect to the same basis and can be interpreted as probability distributions.

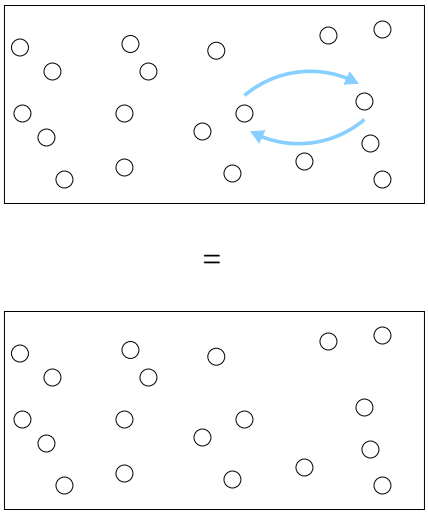

FIG. 2: If the subsystems of a multi-partite system are indistinguishable then its state is symmetric, i.e., invariant under reordering of the subsystems.

can be estimated to any desired accuracy. The tomography problem described above (cf. Fig. 1) can thus be solved under the assumption that the state of the system is i.i.d. This assumption, however, is mostly impossible to justify for realistic systems. In particular, there is no experiment on n subsystems providing enough data to exclude the possibility that there exist correlations involving $N > n$ subsystems (see also Example 2 below).

The state ρ^N of an N-partite system is called *symmetric* if it is invariant under swappings of its subsystems, i.e., formally $\pi\rho^N\pi^\dagger = \rho^N$, where π is an arbitrary permutation (cf. Fig. 2). This is equivalent to say that the order in which the subsystems are represented mathematically is independent of their physical properties. Note that any i.i.d. state is symmetric, whereas the opposite implication does generally not hold. Moreover, for realistic systems, symmetry often follows from certain natural properties such as the indistinguishability of its subsystems. Finally, in practical applications, symmetry can sometimes be *enforced* by randomly permuting the subsystems (as illustrated below).

III. RELATION BETWEEN SYMMETRY AND INDEPENDENCE

As discussed above, the i.i.d. property is strong enough to enable applications such as tomography. However, for real physical systems, it is often only possible to justify symmetry. This raises the question whether symmetry of a physical state still implies a certain similarity to i.i.d. states. The Italian mathematician Bruno de Finetti was the first to study this question for the case of classical probabilistic systems [dF37, MC93].[2] In its generalised form *de Finetti's representation theorem* states the following [DF80]: If the state ρ^N of a classical N-partite system is symmetric, then the state ρ^n of any n-partite subsystem, for $n \ll N$, is approximated by a probabilistic mixture of i.i.d. states $\sigma^{\otimes n}$.[3] Note that, physically, this probabilistic mixture can be interpreted as *one single* i.i.d. state $\sigma^{\otimes n}$ whose prototype σ is unknown.

Later, de Finetti's representation theorem was extended to quantum theory [Stø69, HM76, FLV88, RW89, Pet90, CFS02]. In particular, it has been shown that the statement above holds for any quantum system with finite-dimensional subsystems [KR05, CKMR07] as well as for certain systems with infinite-dimensional subsystems [DOS06]. Furthermore, some of these results have been transformed via Choi-Jamiołkowski isomorphism into statements about completely positive maps (CPMs), which are used to characterise a system's dynamics [FSS04]. De Finetti's representation of symmetric states in terms of i.i.d. states is, however, inherently limited to the case where $n \ll N$. That is, given a large N-partite symmetric state, the i.i.d. property generally only holds approximatively for a small n-partite subsystem [DF80] (see Fig. 3), and the error in the approximation is generally proportional to $\frac{n}{N}$.

To overcome this limitation, we propose a slightly relaxed variant of the i.i.d. property where, roughly speaking, *most*—but not all—of the subsystems of a composite system are identical and independent copies of each other. We then show the following statement, extending de Finetti's representation theorem (see Fig. 3): Given an N-partite quantum state ρ^N, symmetry of ρ^N implies that any n-partite part ρ^n is almost identical to a probabilistic mixture of states ρ^n_σ that satisfy the relaxed i.i.d. property (with prototype σ), as long as n is slightly smaller than N (e.g., $n \approx N - \sqrt{N}$).

To make this more precise, consider a state ρ^n on an n-partite quantum system as well as a state σ on a single subsystem. Then ρ^n is called $\binom{n}{m}$*-i.i.d. (with prototype* σ*)* if it has the form $\sigma^{\otimes m} \otimes \tilde{\rho}^{n-m}$, up to permutations of the subsystems, where $\tilde{\rho}^{n-m}$ is an arbitrary state on $n-m$ subsystems. Note that, for $m = n$, we retrieve the standard notion of i.i.d. states. Our *global*[4] *representation theorem* can now be formulated as follows (see Appendix A for a more technical statement and Appendix B for a proof; see also [Ren05] for a preliminary version as well as [KM07] for a nice generalisation of the result

[2] More precisely, de Finetti's theorem is formulated for probability distributions of random values. Note that probability distributions are the classical counterparts of density operators in quantum mechanics, i.e., they are representations of a system's state (see also Footnote 1).

[3] De Finetti's original work was concerned with the special case where n is fixed and $N \to \infty$ [dF37].

[4] The term *global* refers to the fact that the statement covers virtually the entire system (see Fig. 3).

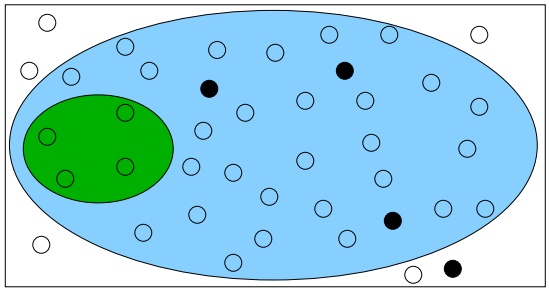

FIG. 3: According to de Finetti's original representation theorem (and its quantum-mechanical analogs), any small part (small oval set) of a large symmetric system satisfies the i.i.d. property. The global representation theorem presented here extends this statement to a set which almost covers the overall system (large oval set), but the i.i.d. property is slightly relaxed in that a small fraction of the subsystems might be in an arbitrary state (black circles).

presented here): Any n-partite part ρ^n of an N-partite symmetric state ρ^N is approximated by a probabilistic mixture of states ρ^n_σ parameterised by σ, where each ρ^n_σ is contained in the space spanned by $\binom{n}{n-r}$-i.i.d. states with prototype σ, for $r \ll n$. The error of the approximation[5] is upper bounded by $\varepsilon = 3e^{-r\frac{N-n}{N}+d\ln(N-n)}$, where d is the dimension of the subsystems, i.e., the decrease is exponential in r.[6] A typical choice for the above parameters is $n := N - N^\alpha$ and $r := N^\alpha$, where $\frac{1}{2} < \alpha < 1$. Roughly speaking, the global representation theorem then says that a symmetric state ρ^N can be seen as a mixture of i.i.d. states, as long as we ignore N^α subsystems and, additionally, tolerate deviations in at most N^α of the subsystems. (Note that N^α is only sublinear in N and the error ε decreases exponentially fast in N.)

IV. EXAMPLES

To get a feel for the above result, we have a look at some examples of symmetric N-partite quantum states. For this, we assume that each subsystem contains a set of d mutually orthogonal (i.e., perfectly distinguishable) states $\{|0\rangle, \ldots, |d-1\rangle\}$ (where $d = 2$ in most examples).

1. Let ρ^N be the uniform mixture of the two N-partite i.i.d. states $|0\rangle^{\otimes N}$ and $|1\rangle^{\otimes N}$. Obviously, any n-partite part ρ^n of ρ^N, for $n \leq N$, still has the same structure, i.e., it is a convex combination of $|0\rangle^{\otimes n}$ and $|1\rangle^{\otimes n}$. For this state, the representation theorem thus holds in a perfect sense (rather than only approximatively). The example illustrates, however, that symmetric states (or parts of them) can generally not be approximated by *one single* i.i.d. state $\sigma^{\otimes n}$, but only by mixtures of such states.

2. Let ρ^N be the uniform mixture of all states $|b_1\rangle \otimes \cdots \otimes |b_N\rangle$ where $(b_1, \cdots b_N) \in \{0,1\}^N$ are N-tuples of binary values with an even number of 1s. Any n-partite part ρ^n, for $n < N$, is equal to the i.i.d. state $\sigma^{\otimes n}$, where σ is the uniform mixture of $|0\rangle$ and $|1\rangle$. Note, however, that ρ^N is not an i.i.d. state. This proves that the i.i.d. property for an N-partite system cannot be verified by any experiment involving less than N subsystems.

3. Let ρ^N be defined by the superposition (with equal amplitudes) of all N-partite states $|b_1\rangle \otimes \cdots \otimes |b_N\rangle$ with an even number of 1s (note the difference to Example 2 where the state is defined by a mixture rather than a superposition of such states). While ρ^N cannot be written as a mixture of i.i.d. states, it is easy to verify that any n-partite part ρ^n, for $n < N$, equals the uniform mixture of the two pure i.i.d. states $|\bar{0}\rangle^{\otimes n}$ and $|\bar{1}\rangle^{\otimes n}$, where $|\bar{0}\rangle := \frac{1}{\sqrt{2}}(|0\rangle + |1\rangle$ and $|\bar{1}\rangle := \frac{1}{\sqrt{2}}(|0\rangle - |1\rangle)$.

4. Let $N = 2$ and let ρ^2 be the bipartite *singlet* state defined by the antisymmetric vector $\frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)$. It is easy to verify that no (mixture of) i.i.d. states $\sigma^{\otimes 2}$ can have an overlap of more than $\frac{1}{4}$ with ρ^2. Because ρ^2 is symmetric[7] the example proves that symmetry is generally weaker than the i.i.d. property. In fact, our representation theorem does not yield any approximation in terms of i.i.d. states because the number of subsystems is small ($N = 2$).

5. Let ρ^N be the N-partite so-called *cat state* defined by $\frac{1}{\sqrt{2}}(|0\rangle^{\otimes N} + |1\rangle^{\otimes N})$. As in the above example, the overlap of any i.i.d. state $\sigma^{\otimes N}$ with ρ^N is upper bounded by $\frac{1}{2}$, i.e., ρ^N cannot be approximated by mixtures of i.i.d. states. However, any n-partite part of ρ^N, for $n < N$, is exactly of the form of Example 1, i.e., a mixture of i.i.d. states.

6. Let ρ^N be defined by the completely antisymmetric vector $\frac{1}{\sqrt{N!}}\sum_\pi \mathrm{sign}(\pi) \cdot \pi(|0\rangle \otimes |1\rangle \otimes \cdots \otimes |N-1\rangle)$ with subsystems of dimension $d = N$. The state ρ^N can be seen as a generalisation of the singlet state of Example 4 (where $N = 2$). Although ρ^N

[5] The error is quantified in terms of the L_1-distance between operators. This distance measure, sometimes called *trace distance*, is motivated by the fact that it corresponds to the probability of successfully distinguishing two quantum states.

[6] If the subsystems are infinite-dimensional, d can usually, for realistic systems, be substituted by some bound on the system's maximum energy.

[7] Note that, although the vector $|\Psi^-\rangle := \frac{1}{\sqrt{2}}(|0\rangle \otimes |1\rangle - |1\rangle \otimes |0\rangle)$ defining the singlet is antisymmetric, i.e., $\pi|\Psi^-\rangle = -|\Psi^-\rangle$, the corresponding physical state $\rho^2 := |\Psi^-\rangle\langle\Psi^-|$ (represented as a density operator) is symmetric, i.e., $\pi\rho^2\pi^\dagger = \rho^2$.

is symmetric, any bipartite part ρ^2 is a mixture of singlet states, and hence cannot be approximated by a mixture of i.i.d. states [CKMR07]. The example thus illustrates that symmetry can only imply independence if the number N of subsystems is sufficiently large compared to the dimension d of the subsystems.

7. Let ρ^N be the uniform mixture of all permutations of the N-partite state $|0\rangle^{\otimes N-1}\otimes|1\rangle$. Obviously, ρ^N is an $\binom{N}{N-1}$-i.i.d. state with prototype $|0\rangle$. However, the distance to any mixture of perfect i.i.d. states is at least $\frac{1}{2}$. This implies that the $\binom{N}{N-r}$-i.i.d. property, for $r > 0$, is strictly weaker than the perfect i.i.d. property.

V. APPLICATIONS

Most physical measures that are used for the characterisation of large composite systems (e.g., the energy or the temperature) are *robust* under disturbances of a small number of subsystems. In particular, their values evaluated for a $\binom{N}{N-r}$-i.i.d. state ρ^N with prototype σ are approximated by their values on the corresponding perfect i.i.d. state $\sigma^{\otimes N}$, as long as $r \ll N$. They are thus fully determined by the prototype state σ (which is the state of a single subsystem). For example, if the measure E is extensive (such as the energy or the entropy) we have $E(\rho^N) \approx E(\sigma^{\otimes N}) = NE(\sigma)$. Furthermore, the prototype state σ can be determined by measurements applied to a limited number of subsystems. Hence, under the assumption that the system's state ρ^N is $\binom{N}{N-r}$-i.i.d. for $r \ll N$, tomography is sufficient to determine the value of any robust physical quantity. The representation theorem outlined in the previous section now implies that the same is still true approximately under the sole assumption that the system's state is symmetric.

A similar reasoning applies to problems in information theory and, in particular, cryptography. A main challenge in these disciplines is to characterise the resources (such as entanglement) which are needed to perform certain tasks (e.g., teleportation). For this, it is often convenient (and very common) to consider resources which consist of many identical and independent parts or, more precisely, to assume that the states describing the resources satisfy the i.i.d. property. It is an immediate consequence of our representation theorem that this assumption can be relaxed to a symmetry assumption. This relaxation is crucial because, in many information-theoretic scenarios, it suffices to consider symmetric states in order to cover the most general case. In fact, symmetry of the states can often be enforced by applying randomly chosen permutations, as illustrated by the following example (see also the Appendix C for an additional example).

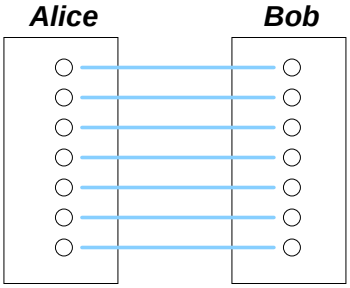

FIG. 4: In the first phase of a QKD scheme, called *distribution phase*, Alice and Bob attempt to distribute a large number of entangled particle pairs, as depicted. In a subsequent *distillation phase*, these are measured locally, resulting in a pair of raw keys held by Alice and Bob, respectively. The raw keys are then processed classically in order to produce a final secret key.

VI. EXAMPLE APPLICATION: SECURITY OF QUANTUM KEY DISTRIBUTION

As indicated above, the global representation theorem has various applications. As an example, we derive a generic result in quantum cryptography [BB84, Eke91]. The result implies security of a large class of quantum key distribution (QKD) schemes against any attack allowed by the laws of quantum physics. Generally speaking, QKD is the art of distributing a (random) secret key to two distant parties, using only communication over an insecure quantum channel as well as an authentic[8] (but public) classical channel. Typical QKD schemes consist of two subsequent phases [Eke91, BBM92]: In a *distribution phase*, one of the parties, traditionally called *Alice*, prepares N entangled particle pairs and sends one half of each pair over the quantum channel to the other party, *Bob* (cf. Fig. 4). Then, in a *distillation phase*, Alice and Bob apply local measurements to their particles, resulting in a pair of correlated classical strings, called *raw keys*; finally, depending on an estimate of the strength of correlation between their respective raw keys, Alice and Bob employ some purely classical procedures to transform them into identical secret keys.[9]

As an adversary might tamper with the particles sent over the (insecure) quantum channel, the joint state ρ^N of the N particle pairs held by Alice and Bob after the distribution phase is generally (almost) arbitrary. Hence, to prove security of the scheme against general attacks, one has to show that the distillation

[8] A communication channel is said to be *authentic* if no adversary can alter the transmitted messages without being detected. Using a short initial key, an authentic channel can be simulated even if only a completely insecure channel is available [Sti05].

[9] The length of the generated keys depends on the correlation between the raw keys and might be zero if this correlation is too weak.

phase works correctly whatever the state ρ^N is. Because the space of possible states ρ^N is exponentially large in N, this analysis is non-trivial and has only been possible for QKD protocols which satisfy certain specific requirements [May96, LC99, SP00].[10] In fact, standard information-theoretic arguments are usually restricted to situations where the state ρ^N is i.i.d., i.e., $\rho^N = \sigma^{\otimes N}$. This, however, is only guaranteed for so-called *collective attacks*, where the adversary is bound to apply the same operation separately to each of the particles sent over the channel [BM97, BBB$^+$02, DW05].

Using the global representation theorem for symmetric states presented in this article, it can be shown that security of a QKD scheme against collective attacks implies security against arbitrary attacks (where no restriction is imposed on the adversary). The argument is based on two observations: (i) The security of the distillation phase only depends on *robust* properties of the state ρ^N of the N particle pairs held by Alice and Bob after the distribution phase, i.e., security is not affected by alterations of a small number of subsystems [Ren05]. (ii) If Alice and Bob both reorder their particles according to a common randomly chosen permutation then the resulting state of the particle pairs (averaged over all possible permutations) is *symmetric*.[11] Now, given a QKD scheme which is provably secure against collective attacks, observation (i) implies that the same scheme is secure whenever the state ρ^N has some n-partite part which is $\binom{n}{n-r}$-i.i.d., where $N - n \ll N$ and $r \ll n$. Hence, by our representation theorem, it suffices to verify that ρ^N is symmetric, which is the case because of observation (ii). We thus get the following result: If a QKD scheme is secure against collective attacks then the same scheme, equipped with an additional randomised permutation step inserted after the distribution phase,[12] is secure against any attack allowed by the laws of quantum physics.[13]

VII. CONCLUSIONS

We have presented a de Finetti style representation theorem which connects two properties that the physical state of a multi-partite system can have: (i) *symmetry:* swappings of the subsystems leave the state unchanged; (ii) *i.i.d.:* the individual parts of the state are identical and mutually independent. The theorem states that symmetry of a large system implies that the i.i.d. property approximately holds on almost the entire system.

The i.i.d. property is often employed for the study of large systems, but cannot usually be verified directly. In contrast, the symmetry property is, for example, implied by the indistinguishability of the subsystems or can be enforced by a random permutation. As the representation theorem connects these two properties, it has implications within various areas of physics (as does de Finetti's original theorem, which is used, e.g., in mathematical physics and statistical mechanics [FSV80, FLV88, RW89]). Furthermore, the theorem has consequences for quantum information theory. For instance, as demonstrated above, it implies that the security of a QKD scheme against general attacks follows directly from its security against collective attacks (which can be proved using standard information-theoretic arguments).

The connection between symmetric and i.i.d. states is of particular interest for foundational issues [Hud81, CFS02]. As discussed above, it implies that symmetry suffices to predict physical properties of a large quantum system given only data obtained from the observation of a limited number of subsystems. Since the ability to make predictions is crucial in physics, one might go one step further and postulate that a similar statement should be true within any reasonable physical theory (other than quantum mechanics). Such a postulate would indeed restrict the space of possible theories. For example, within a theory where physical states are represented as vectors in a real Hilbert space, even de Finetti's original representation theorem cannot hold [CFS02].

Acknowledgments

I would like to thank Charles Bennett, Matthias Christandl, Artur Ekert, Robert König, Ueli Maurer, and Graeme Mitchison for their valuable and very helpful comments on earlier versions of this work. This research is supported by HP Labs Bristol as well as by the European Union through the Integrated Projects QAP (IST-3-015848), SCALA (CT-015714), SECOQC and the QIP IRC (GR/S821176/01).

APPENDIX A: TECHNICAL STATEMENT OF THE REPRESENTATION THEOREM

Let $\mathcal{H}$ be a d-dimensional Hilbert space. The *symmetric subspace of* $\mathcal{H}^{\otimes n}$, denoted $\mathrm{Sym}^n(\mathcal{H})$, is the space spanned by all vectors which are invariant under permutations of the n subsystems. Formally, let S_n be the set of permutations on $\{1, \ldots, n\}$. For any $\pi \in S_n$, we also write π to denote the unitary on $\mathcal{H}^{\otimes n}$ which maps any product vector $\phi_1 \otimes \cdots \otimes \phi_n$ to $\phi_{\pi^{-1}(1)} \otimes \cdots \otimes \phi_{\pi^{-1}(n)}$. Then $\mathrm{Sym}^n(\mathcal{H}) := \{\Psi \in \mathcal{H}^{\otimes n} : \pi\Psi = \Psi, \forall \pi \in S_n\}$.

[10] A typical requirement is that the protocol can be translated into a certain entanglement purification scheme [BBP$^+$96].

[11] Note that this holds even if the permutation is known to the adversary.

[12] Inserting such a symmetrisation step is, however, only necessary if the scheme is not symmetric. In fact, many schemes are already symmetric by construction (see, e.g., [DEJ$^+$96]).

[13] This solves an open question originally raised by Biham and Mor [BM97].

Let ν be a rank-one projector on $\mathcal{H}$. A vector $\Psi \in \mathcal{H}^{\otimes n}$ is called $\binom{n}{m}$-*i.i.d.* in ν if there exists a permutation $\pi \in S_n$ such that $(\nu^{\otimes m} \otimes \mathrm{id}^{\otimes n-m})\pi\Psi = \pi\Psi$. Intuitively, this means that the state defined by the vector Ψ is of the form ν on (at least) m subsystems.

Our main result establishes a connection between the symmetry and the i.i.d. property as defined above.

Theorem 1. *Let $n, k, r \in \mathbb{N}$ and let $\mathcal{H}$ be a d-dimensional Hilbert space. For any density operator ρ^{n+k} on $\mathrm{Sym}^{n+k}(\mathcal{H})$ there exists a measure $d\nu$ on the set $\mathcal{V}$ of one-dimensional projectors on $\mathcal{H}$ and a family of density operators ρ_ν^n on $\mathrm{Sym}^n(\mathcal{H})$ such that, for any $\nu \in \mathcal{V}$, ρ_ν^n has support on the space spanned by all $\binom{n}{n-r}$-i.i.d. vectors in ν and*

$$\left\|\mathrm{tr}_k(\rho^{n+k}) - \int \rho_\nu^n d\nu\right\|_1 \leq 3e^{-\frac{k(r+1)}{n+k}+d\ln k} \ .$$

Furthermore, if ρ^{n+k} has rank one then the same is true for the operators ρ_ν^n.

For any $N \in \mathbb{N}$, let ρ^N be a density operator on $\mathrm{Sym}^N(\mathcal{H})$ and let $\varepsilon > 0$ be fixed. If we apply Theorem 1 with $k := \lceil \varepsilon N \rceil$, $r := \lceil \varepsilon N \rceil$, and $n := N - k$, then the error in the approximation provided by Theorem 1 decreases exponentially fast in N. Hence, very roughly speaking, the state ρ^N is exponentially (in N) close to a mixture of states which are i.i.d. except on an arbitrarily small fraction (namely $r+k = 2\varepsilon N$) of the N subsystems.

Note that a density operator ρ^N on $\mathcal{H}^{\otimes N}$ which is symmetric under permutations, i.e., $\pi\rho^N\pi^\dagger = \rho^N$ for any $\pi \in S_N$, cannot necessarily be seen as an operator on $\mathrm{Sym}^N(\mathcal{H})$.[14] Hence, in order to apply Theorem 1 to general symmetric quantum states, we need an additional lemma. It says that any permutation-invariant operator has a purification on a symmetric subspace [Ren05, CKMR07].

Lemma 2. *Let ρ^N be a nonnegative operator on $\mathcal{H}^{\otimes N}$ such that $\pi\rho^N\pi^\dagger = \rho^N$, for any $\pi \in S_N$. Then there exists a rank-one operator $\bar{\rho}^N$ on $\mathrm{Sym}^N(\mathcal{H} \otimes \mathcal{K}) \subseteq (\mathcal{H} \otimes \mathcal{K})^{\otimes N}$, where $\mathcal{K} \cong \mathcal{H}$, such that $\rho^N = \mathrm{tr}_{\mathcal{K}^{\otimes N}}(\bar{\rho}^N)$.*

APPENDIX B: PROOF OF THE REPRESENTATION THEOREM

The proof of Theorem 1 is based on three technical lemmas (Lemma 3–5). The first can be seen as a variant of Winter's gentle measurement lemma [Win99] and is implicitly used in related work [CKMR07].

[14] A simple example illustrating this fact is the operator $\rho^N = \frac{1}{d^N}\mathrm{id}_{\mathcal{H}^{\otimes N}}$.

Lemma 3. *Let $\{\rho_\tau\}_{\tau\in\mathcal{T}}$ be a family of nonnegative operators on a Hilbert space $\mathcal{H}$ and let $\{P_\tau\}_{\tau\in\mathcal{T}}$ be a family of projectors on $\mathcal{H}$. Then, for any measure $d\tau$ on $\mathcal{T}$,*

$$\left\|\int (\rho_\tau - P_\tau\rho_\tau P_\tau)d\tau\right\|_1 \leq 3\left\|\int (\mathrm{id} - P_\tau)\rho_\tau d\tau\right\|_1 \ .$$

Proof. Using the identity

$$\begin{aligned}&\rho_\tau - P_\tau\rho_\tau P_\tau \\ &= (\mathrm{id} - P_\tau)\rho_\tau + \rho_\tau(\mathrm{id} - P_\tau) - (\mathrm{id} - P_\tau)\rho_\tau(\mathrm{id} - P_\tau) \ ,\end{aligned}$$

the triangle inequality, and the fact that $\|A\|_1 = \|A^\dagger\|_1$ holds for any operator A, we find

$$\left\|\int (\rho_\tau - P_\tau\rho_\tau P_\tau)d\tau\right\|_1 \leq 2\alpha + \beta \qquad \text{(B1)}$$

where

$$\begin{aligned}\alpha &:= \left\|\int (\mathrm{id} - P_\tau)\rho_\tau d\tau\right\|_1 \\ \beta &:= \left\|\int (\mathrm{id} - P_\tau)\rho_\tau(\mathrm{id} - P_\tau)d\tau\right\|_1 \ .\end{aligned}$$

Because, for any $\tau \in \mathcal{T}$, the operator $(\mathrm{id} - P_\tau)\rho_\tau(\mathrm{id} - P_\tau)$ is nonnegative, the norm in the definition of β can be replaced by a trace, that is,

$$\begin{aligned}\beta &= \mathrm{tr}\Big(\int (\mathrm{id} - P_\tau)\rho_\tau(\mathrm{id} - P_\tau)d\tau\Big) \\ &= \mathrm{tr}\Big(\int (\mathrm{id} - P_\tau)\rho_\tau d\tau\Big) \ ,\end{aligned}$$

where the second equality follows from the cyclicity of the trace and the fact that $P_\tau P_\tau = P_\tau$. Because $\mathrm{tr}(A) \leq \|A\|_1$ holds for any operator A, we conclude that $\beta \leq \alpha$. The statement then follows from (B1). □

The next lemma is derived using basic arguments from representation theory.

Lemma 4. *Let A be an operator on $\mathcal{H}^{\otimes n}$ and define*

$$\Gamma := \frac{\dim(\mathrm{Sym}^n(\mathcal{H}))}{\mathrm{tr}(P_{\mathrm{Sym}^n(\mathcal{H})}A)} \int U^{\otimes n} A (U^\dagger)^{\otimes n} dU$$

where dU is the normalised Haar measure on the set of unitaries $\mathcal{U}(\mathcal{H})$. Then

$$\Gamma P_{\mathrm{Sym}^n(\mathcal{H})} = P_{\mathrm{Sym}^n(\mathcal{H})} \ ,$$

where $P_{\mathrm{Sym}^n(\mathcal{H})}$ is the projector onto the symmetric subspace of $\mathcal{H}^{\otimes n}$.

Proof. The space $\mathcal{H}^{\otimes n}$ can be decomposed into subspaces $\mathcal{H}_\lambda$ labelled by Young diagrams λ with n boxes and at most $d := \dim(\mathcal{H})$ rows, i.e., $\mathcal{H}^{\otimes n} \cong \bigoplus_\lambda \mathcal{H}_\lambda^{\oplus m_\lambda}$, for some $m_\lambda \in \mathbb{N}$, such that the following holds. Let τ be the mapping from $\mathcal{U}(\mathcal{H})$ to $\mathcal{H}^{\otimes n}$ defined by $V \mapsto V^{\otimes n}$ and let P_λ be the projector onto any of the subspaces $\mathcal{H}_\lambda$ with

Young diagram λ. Then P_λ commutes with $\tau(V)$, for any $V \in \mathcal{U}(\mathcal{H})$, and $V \mapsto P_\lambda \tau(V)$ is an irreducible representation of $\mathcal{U}(\mathcal{H})$. Furthermore, two such representations are equivalent if and only if their Young diagrams λ are identical.

Because dU is the Haar measure, the operator Γ commutes with $\tau(V)$, i.e., $\tau(V)\Gamma = \Gamma\tau(V)$, for any $V \in \mathcal{U}(\mathcal{H})$. Let P_λ and $P'_{\lambda'}$ be two projectors onto any of the subspaces $\mathcal{H}_\lambda$ and $\mathcal{H}_{\lambda'}$, respectively, as defined by the above decomposition. Since these projectors commute with $\tau(V)$, we have

$$(P_\lambda \tau(V))(P_\lambda \Gamma P'_{\lambda'}) = (P_\lambda \Gamma P'_{\lambda'})(P'_{\lambda'} \tau(V)) \ ,$$

for all $V \in \mathcal{U}(\mathcal{H})$. Consequently, by Schur's lemma, the operator $P_\lambda \Gamma P'_{\lambda'}$ acts like a scalar on $\mathcal{H}_\lambda$ if $\lambda = \lambda'$ and equals zero otherwise. In particular, because for the Young diagram $\lambda = (n)$ with n boxes and one row $m_\lambda = 1$ and $P_\lambda = P_{\mathrm{Sym}^n(\mathcal{H})}$ holds, we find

$$\begin{aligned} \Gamma P_{\mathrm{Sym}^n(\mathcal{H})} &= P_{\mathrm{Sym}^n(\mathcal{H})} \Gamma P_{\mathrm{Sym}^n(\mathcal{H})} + P^\perp_{\mathrm{Sym}^n(\mathcal{H})} \Gamma P_{\mathrm{Sym}^n(\mathcal{H})} \\ &= \gamma \cdot P_{\mathrm{Sym}^n(\mathcal{H})} \ , \end{aligned}$$

for some $\gamma \in \mathbb{R}$. Taking the trace on both sides of the equality gives $\gamma = 1$. □

Finally, we need an explicit basis of the symmetric subspace $\mathrm{Sym}^n(\mathcal{H})$.

Lemma 5. *Let $\mathcal{H}$ be a d-dimensional Hilbert space with orthonormal basis $\{\omega_b\}_{b\in[d]}$, where $[d] := \{1, \ldots, d\}$, and let $n \in \mathbb{N}$. Let Λ^n_d be the set of d-tuples $\lambda = (\lambda_1, \ldots, \lambda_d) \in \mathbb{N}^d$ such that $\sum_{b=1}^d \lambda_b = n$, and, for any $\lambda \in \Lambda^n_d$, let $\mathcal{B}_\lambda$ be the set of n-tuples $(b_1, \ldots, b_n) \in [d]^n$ such that $|\{i : b_i = b\}| = \lambda_b$ for $b \in [d]$. Then the family $\{\Phi_\lambda\}_{\lambda\in\Lambda^n_d}$ of vectors $\Phi_\lambda \in \mathcal{H}^{\otimes n}$ defined by*

$$\Phi_\lambda := \sqrt{\frac{1}{|\mathcal{B}_\lambda|}} \sum_{b\in\mathcal{B}_\lambda} \omega_{b_1} \otimes \cdots \otimes \omega_{b_n}$$

is an orthonormal basis of $\mathrm{Sym}^n(\mathcal{H})$. In particular, $\dim(\mathrm{Sym}^n(\mathcal{H})) = \|\Lambda^n_d\| = \binom{n+d-1}{n}$.

Proof. See the standard literature on representation theory [FH91]. □

Proof of Theorem 1. Let ν_0 be a fixed one-dimensional projector in $\mathcal{H}$. For $n, r \in \mathbb{N}$ and any unitary $U \in \mathcal{U}(\mathcal{H})$, let $P_U^{n,r}$ be the projector onto the subspace of $\mathcal{H}^{\otimes n}$ spanned by all $\binom{n}{n-r}$-i.i.d. vectors in $\nu := U\nu_0 U^\dagger$. In particular,

$$P_U^{n,r} = U^{\otimes n} P^{n,r}_{\mathrm{id}} (U^\dagger)^{\otimes n} \ . \tag{B2}$$

Define

$$\begin{aligned} \rho^n_U &:= \dim(\mathrm{Sym}^k(\mathcal{H})) \cdot \mathrm{tr}_k\big(\mathrm{id}^{\otimes n} \otimes P^{k,0}_U \cdot \rho^{n+k}\big) \\ \bar\rho^n_U &:= P_U^{n,r} \rho^n_U P_U^{n,r} \ , \end{aligned}$$

where tr_k denotes the partial trace over the last k subsystems, and let dU be the normalised Haar measure on $\mathcal{U}(\mathcal{H})$. It is straightforward to verify that $\bar\rho^n_U$ is a nonnegative operator. Moreover, because $P^{k,0}_U$ and ρ^{n+k} have rank one, $\bar\rho^n_U$ has rank one as well. Since, by definition, $\bar\rho^n_U$ has support on the subspace containing all $\binom{n}{n-r}$-i.i.d. vectors in $\nu := U\nu_0 U^\dagger$, it suffices to show that

$$\delta := \Big\| \mathrm{tr}_k(\rho^{n+k}) - \int \bar\rho^n_U dU \Big\|_1 \leq 3e^{-\frac{k(r+1)}{n+k} + d\ln k} \ . \tag{B3}$$

Using (B2) together with the fact that $P^{k,0}_{\mathrm{id}}$ has support on the symmetric subspace $\mathrm{Sym}^k(\mathcal{H})$ and trace equal to one, we can apply Lemma 4 which gives

$$\dim(\mathrm{Sym}^k(\mathcal{H})) \int P^{k,0}_U dU \cdot P_{\mathrm{Sym}^k(\mathcal{H})} = P_{\mathrm{Sym}^k(\mathcal{H})} \ .$$

Since, by assumption, ρ^{n+k} has support on $\mathrm{Sym}^{n+k}(\mathcal{H}) \subseteq \mathcal{H}^{\otimes n} \otimes \mathrm{Sym}^k(\mathcal{H})$, we conclude

$$\mathrm{tr}_k(\rho^{n+k}) = \int \rho^n_U dU \ .$$

The distance δ can thus be rewritten as

$$\delta = \Big\| \int (\rho^n_U - P_U^{n,r} \rho^n_U P_U^{n,r}) dU \Big\|_1 \ .$$

Let $(P_U^{n,r})^\perp := \mathrm{id}_{\mathcal{H}^{\otimes n}} - P_U^{n,r}$ be the projector orthogonal to $P_U^{n,r}$. By Lemma 3, we have

$$\begin{aligned} \delta &\leq 3 \Big\| \int (P_U^{n,r})^\perp \rho^n_U dU \Big\|_1 \\ &= 3 \dim(\mathrm{Sym}^k(\mathcal{H})) \cdot \big\| \mathrm{tr}_k(\Gamma^{n+k} \rho^{n+k}) \big\|_1 \end{aligned} \tag{B4}$$

where

$$\Gamma^{n+k} := \int (P_U^{n,r})^\perp \otimes P^{k,0}_U dU \ .$$

Using again the fact that ρ^{n+k} has support on $\mathrm{Sym}^{n+k}(\mathcal{H})$ together with identity (B2) and Lemma 4, the norm on the r.h.s. of (B4) can be rewritten as

$$\begin{aligned} \big\| \mathrm{tr}_k(\Gamma^{n+k} \rho^{n+k}) \big\|_1 &= \big\| \mathrm{tr}_k(\Gamma^{n+k} P_{\mathrm{Sym}^{n+k}(\mathcal{H})} \rho^{n+k}) \big\|_1 \\ &= \gamma \cdot \mathrm{tr}(P_{\mathrm{Sym}^{n+k}(\mathcal{H})} \rho^{n+k}) = \gamma \ , \end{aligned}$$

where

$$\gamma := \frac{\mathrm{tr}\big(P_{\mathrm{Sym}^{n+k}(\mathcal{H})} (P_{\mathrm{id}}^{n,r})^\perp \otimes P^{k,0}_{\mathrm{id}}\big)}{\dim(\mathrm{Sym}^{n+k}(\mathcal{H}))} \ .$$

In order to show that (B3) holds, we insert this into (B4). Because $\dim(\mathrm{Sym}^k(\mathcal{H})) = \binom{k+d-1}{k}$ (cf. Lemma 5) and $\binom{k+d-1}{k} \leq k^d$, for $k \geq 2$ (note that the statement of the theorem is trivial for $k = 1$), it remains to verify that

$$\gamma \leq e^{-\frac{k(r+1)}{n+k}} \ . \tag{B5}$$

Let $\{\omega_b\}_{b\in[d]}$ be an orthonormal basis of $\mathcal{H}$ such that ω_b, for $b = d$, is contained in the support of ν_0. Furthermore, let Λ_d^{n+k} and $\{\Phi_\lambda\}_{\lambda\in\Lambda_d^{n+k}}$ be defined as in Lemma 5, such that the latter is a basis of $\mathrm{Sym}^{n+k}(\mathcal{H})$. Then γ can be rewritten as

$$\gamma = \frac{1}{|\Lambda_d^{n+k}|}\sum_{\lambda\in\Lambda_d^{n+k}} \Phi_\lambda^\dagger (P_{\mathrm{id}}^{n,r})^\perp \otimes P_{\mathrm{id}}^{k,0}\Phi_\lambda \ .$$

A straightforward calculation shows that, for any $\lambda \in \Lambda_d^{n+k}$ and $s := \sum_{b=1}^{d-1}\lambda_b$,

$$\Phi_\lambda^\dagger (P_{\mathrm{id}}^{n,r})^\perp \otimes P_{\mathrm{id}}^{k,0}\Phi_\lambda = \begin{cases} 0 & \text{if } s \le r \\ \frac{(n+k-s)!n!}{(n+k)!(n-s)!} & \text{otherwise.}\end{cases}$$

This immediately gives an upper bound on γ,

$$\gamma \le \frac{(n+k-r-1)!n!}{(n+k)!(n-r-1)!} \le \Big(\frac{n}{n+k}\Big)^{r+1} \ .$$

Using the fact that, for any $\beta \in [0,1]$, $(1-\beta)^{1/\beta} \le e^{-1}$, we find, with $\beta := \frac{k}{n+k}$,

$$\frac{n}{n+k} = \big((1-\beta)^{1/\beta}\big)^\beta \le e^{-\frac{k}{n+k}} \ .$$

This implies (B5) and thus concludes the proof. □

APPENDIX C: EVALUATING EXTENSIVE QUANTITIES ON SYMMETRIC STATES

In the following, we show that the global representation theorem (Theorem 1) can be used to derive structural properties of extensive quantities. In particular, we prove the following proposition.

Proposition 1 (Informal Proposition)**.** *Let E be a concave extensive quantity which is continuous and robust (such that the variation of E when altering k subsystems is proportional to k). Then, for any family of symmetric states ρ^N on $\mathcal{H}^{\otimes N}$ parameterised by $N \in \mathbb{N}$,*

$$\lim_{N\to\infty}\frac{1}{N}E(\rho^N) \ge \min_\sigma E(\sigma) \ . \tag{C1}$$

Typical examples of quantities satisfying the assumptions of the proposition are entropy measures, including the *von Neumann entropy*, and entanglement measures (see also [Ren05]).

Proof sketch. Let $d := \dim(\mathcal{H})$, $k := N^{2/3}$, $r := N^{2/3}$, and define $\rho^n := \mathrm{tr}_k(\rho^N)$, where $n = N - k$. According to Theorem 1, there exists a measure $d\sigma$ on the set of projectors on $\mathcal{H}$ such that

$$\big\|\rho^n - \int \rho_\sigma^n d\sigma\big\|_1 \le \delta := 3e^{-N^{1/3}+d\ln(N)}$$

where, for any σ, ρ_σ^n has support on the space spanned by $\binom{n}{r}$-i.i.d. vectors in σ. Hence, using the continuity of E,

$$E(\rho^n) \approx E\Big(\int \rho_\sigma^n d\sigma\Big) \ .$$

Furthermore, by the concavity of E,

$$E\Big(\int \rho_\sigma^n d\sigma\Big) \ge \int E(\rho_\sigma^n)d\sigma \ge \min_\sigma E(\rho_\sigma^n) \ .$$

Combining this with the above and using the robustness of E, we find

$$E(\rho^N) \approx E(\rho^n) \gtrapprox \min_\sigma E(\rho_\sigma^n) \ .$$

Because ρ_σ^n has support on the space of $\binom{n}{r}$-i.i.d. states in σ, robustness implies $E(\rho_\sigma^n) \approx E(\sigma^{\otimes n})$. The statement then follows from the fact that E is extensive, i.e., $E(\sigma^{\otimes n}) = nE(\sigma)$, and $\frac{n}{N} \approx 1$. □

Proposition 1 provides some insights into a well-known problem of quantum information theory. Essentially, the problem is to prove the following conjecture, called *additivity of the minimum output entropy of a quantum channel* [Sho04].

Conjecture 1. *For any trace-preserving completely positive map (CPM) $\mathcal{E}$, the von Neumann entropy S of the outcome of $\mathcal{E}$, minimised over all possible inputs, is an extensive quantity.*

For a proof of this conjecture, it has to be shown that

$$\frac{1}{N}S(\mathcal{E}^{\otimes N}(\rho^N)) \ge \min_\sigma S(\mathcal{E}(\sigma)) \tag{C2}$$

holds for any density operator ρ^N on $\mathcal{H}^{\otimes N}$. In the special case where ρ^N is symmetric, an asymptotic version of (C2) follows from Proposition 1. To see this, it suffices to verify that the function E defined by $E(\rho^N) := S(\mathcal{E}^{\otimes N}(\rho^N))$ satisfies the assumptions of the proposition, which is straightforward.

[BB84] C. H. Bennett and G. Brassard. Quantum cryptography: Public-key distribution and coin tossing. In *Proceedings of IEEE International Conference on Computers, Systems and Signal Processing*, pages 175–179, 1984.

[BBB+02] E. Biham, M. Boyer, G. Brassard, J. van de Graaf, and T. Mor. Security of quantum key distribution against all collective attacks. *Algorithmica*, 34:372–388, 2002.

[BBM92] C. H. Bennett, G. Brassard, and N. D. Mermin. Quantum cryptography without Bell's theorem. *Phys. Rev. Lett.*, 68:557–559, 1992.

[BBP+96] C. H. Bennett, G. Brassard, S. Popescu, B. Schumacher, J. Smolin, and W. Wootters. Purification of noisy entanglement and faithful teleportation via noisy channels. *Phys. Rev. Lett.*, 76:722–726, 1996.

[BM97] E. Biham and T. Mor. Security of quantum cryptography against collective attacks. *Phys. Rev. Lett.*, 78(11):2256–2259, 1997.

[CFS02] C. M. Caves, C. A. Fuchs, and R. Schack. Unknown quantum states: The quantum de Finetti representation. *J. Math. Phys.*, 43:4537, 2002.

[CKMR07] M. Christandl, R. König, G. Mitchison, and R. Renner. One-and-a-half quantum de Finetti theorems. *Comm. Math. Phys.*, 2007. to appear.

[DEJ+96] D. Deutsch, A. Ekert, R. Jozsa, C. Macchiavello, S. Popescu, and A. Sanpera. Quantum privacy amplification and the security of quantum cryptography over noisy channels. *Phys.Rev.Lett.*, 77:2818–2821, 1996.

[dF37] B. de Finetti. La prévision: ses lois logiques, ses sources subjectives. *Ann. Inst. H. Poincaré*, 7:1–68, 1937.

[DF80] P. Diaconis and D. Freedman. Finite exchangeable sequences. *The Annals of Probability*, 8(4):745–764, 1980.

[DOS06] C. D'Cruz, T. Osborne, and R. Schack. A finite de Finetti theorem for infinite-dimensional systems. `http://arxiv.org/abs/quant-ph/0606139`, 2006.

[DW05] I. Devetak and A. Winter. Distillation of secret key and entanglement from quantum states. *Proc. R. Soc. Lond. A*, 461:207–235, 2005.

[Eke91] A. K. Ekert. Quantum cryptography based on Bell's theorem. *Phys. Rev. Lett.*, 67:661–663, 1991.

[FH91] W. Fulton and J. Harris. *Representation Theory, A First Course*. Springer, 1991.

[FLV88] M. Fannes, J. T. Lewis, and A. Verbeure. Symmetric states of composite systems. *Lett. Math. Phys.*, 15:255–260, 1988.

[FSS04] C. A. Fuchs, R. Schack, and P. F. Scudo. A de Finetti representation theorem for quantum process tomography. *Phys. Rev. A*, 69:062305, 2004.

[FSV80] M. Fannes, H. Spohn, and A. Verbeure. Equilibrium states for mean field models. *J. Math. Phys.*, 21(2):355–358, 1980.

[HM76] R. L. Hudson and G. R. Moody. Locally normal symmetric states and an analogue of de Finetti's theorem. *Z. Wahrschein. verw. Geb.*, 33:343–351, 1976.

[Hud81] R. L. Hudson. Analogs of de Finetti's theorem and interpretative problems of quantum mechanics. *Found. Phys.*, 11:805–808, 1981.

[KM07] R. König and G. Mitchison. Weight spaces and "exponential" quantum de Finetti theorems. Manuscript. 2007.

[KR05] R. König and R. Renner. A de Finetti representation for finite symmetric quantum states. *J. Math. Phys.*, 46:122108, 2005.

[LC99] H.-K. Lo and H. F. Chau. Unconditional security of quantum key distribution over arbitrarily long distances. *Science*, 283:2050–2056, 1999.

[May96] D. Mayers. Quantum key distribution and string oblivious transfer in noisy channels. In *Advances in Cryptology — CRYPTO '96*, volume 1109 of *Lecture Notes in Computer Science*, pages 343–357. Springer, 1996.

[MC93] P. Monari and D. Cocchi, editors. *Introduction to Bruno de Finetti's "Probabiliá e Induzione"*. Cooperativa Libraria Universitaria Editrice, Bologna, 1993.

[Pet90] D. Petz. A de Finetti-type theorem with m-dependent states. *Prob. Th. Rel. Fields.*, 85(1), 1990.

[Ren05] R. Renner. *Security of Quantum Key Distribution*. PhD thesis, Swiss Federal Institute of Technology (ETH) Zurich, 2005. Available at `http://arxiv.org/abs/quant-ph/0512258`.

[RW89] G. A. Raggio and R. F. Werner. Quantum statistical mechanics of general mean field systems. *Helv. Phys. Acta*, 62:980–1003, 1989.

[Sho04] P. W. Shor. Equivalence of additivity questions in quantum information theory. *Comm. Math. Phys.*, 246(3):453–472, 2004.

[SP00] P. W. Shor and J. Preskill. Simple proof of security of the BB84 quantum key distribution protocol. *Phys. Rev. Lett.*, 85:441, 2000.

[Sti05] D. R. Stinson. *Cryptography: Theory and Practice, Third Edition*, volume 36 of *Discrete Mathematics and Its Applications*. CRC Press, 2005.

[Stø69] E. Størmer. Symmetric states of infinite tensor products of C^*-algebras. *J. Funct. Anal.*, 3:48–68, 1969.

[Win99] A. Winter. Coding theorem and strong converse for quantum channels. *IEEE Trans. Inf. Th.*, 45(7), 1999.